

EXECUTIVE SECRETARIAT
ROUTING SLIP

TO:

		ACTION	INFO	DATE	INITIAL
1	DCI				
2	DDCI				
3	EXDIR		X		
4	D/ICS		X (for SECOM)		
5	DDI				
6	DDA		X (for D/OC & D/OIT)		
7	DDO				
8	DDS&T				
9	Chm/NIC				
10	GC				
11	IG				
12	Compt				
13	D/Pers				
14	D/OLL				
15	D/PAO				
16	SA/IA				
17	AO/DCI				
18	C/IPD/OIS				
19	NIO				
20					
21					
22					
SUSPENSE		Date			

Remarks

STAT

Executive Secretary

18 Apr 85

Date

3637 (10-81)

NTISSC

NATIONAL
TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY
COMMITTEE

OFFICE OF THE EXECUTIVE SECRETARY

NTISSC 18-85
9 April 1985

LOGGED

19 APR 1985

Comm

**MEMORANDUM FOR THE MEMBERS AND OBSERVERS, NATIONAL TELECOMMUNICATIONS
AND INFORMATION SYSTEMS SECURITY COMMITTEE**

SUBJECT: NTISS Instruction 40001, Controlled Cryptographic Items (CCI)

Comments received from the Committee were carefully considered by the NSA and most were accommodated. The Instruction with the accepted modifications was signed by the National Manager on 25 March 1985 (copy attached).

The main topic addressed in the comments received focused on the CCI accounting system, its impact on organizations and the system's flexibility. The NSA recognizes that any new system or modification to an existing system causes some difficulty in implementation, but the NSA is committed to assisting those affected departments and agencies in the implementation of the accounting system. Of the remaining comments, three were identified by the NSA as particularly significant items. They include:

First, promulgating the NTISS Instruction through the Secretary of Defense rather than the National Manager. This was proposed based on the NSDD 145, paragraph 6., which states that the Secretary of Defense as the Executive Agent is "responsible for implementing, under his signature, policies developed by the NTISSC." This subject was also discussed at the first NTISSC meeting held on 8 November 1984.

The proposal was not adopted since the National Manager, in the name of the Executive Agent, has the authority under NSDD 145, to "prescribe the minimum standards, methods and procedures for protecting cryptographic and other sensitive technical security material, techniques and information." This is accomplished through a NTISS Instruction vice a NTISS Policy which is promulgated by the Executive Agent or, under the provision of NTISS Directive 900, Annex B paragraph 1., the Chairman of the Steering Group or the Chairman of the NTISSC.

Secondly, the determination that the NTISS Instruction creates a new category of unclassified, but controlled, COMSEC equipment which would modify current national policies and that such modifications needed to be discussed at the NTISSC level.

The Instruction, in focusing on a new category of cryptographic items, does not constitute a new policy or a modification to an existing policy. Rather, it provides a definition and handling procedures for the equipment which is already governed by existing national policy.

Thirdly, a recommendation was offered to allow foreign national access to CCI equipment as a part of the normal handling procedures used in logistics channels at overseas locations. The basic requirement restricting "access" to U.S. citizens and to resident aliens who are U.S. Government civilian or military

personnel whose duties require access, must remain intact to ensure the integrity of the equipment to the user. The NSA is reviewing the logistics issue and is working to provide some relief to the services.

All Committee comments and recommendations are held in the NTISSC Secretariat and are available to you for your review.

STAT



Executive Secretary

Encl:
a/s

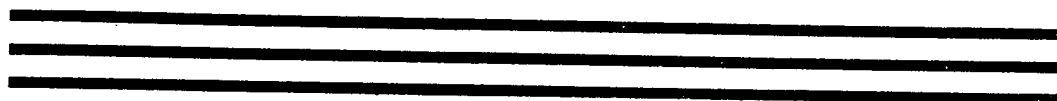


NTISSI NO. 4001
DATE: 25 March 85



NTISS

NATIONAL
TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY



**CONTROLLED
CRYPTOGRAPHIC ITEMS**

FOR OFFICIAL USE ONLY

NTISS
NATIONAL
TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY

NATIONAL MANAGER

FOREWORD

1. National Telecommunications and Information Systems Security Instruction (NTISSI) No. 4001, "Controlled Cryptographic Items," establishes a new category of secure telecommunications and information handling equipments, and associated cryptographic components, which are unclassified but controlled. This Instruction also prescribes the requirements for controlling the new category of equipments and components.


2. This Instruction is effective immediately. Additional copies may be obtained from:

Executive Secretariat
National Telecommunications and Information
Systems Security Committee
National Security Agency
Fort George G. Meade, Maryland 20755-6000

3. This Instruction is not releasable to foreign nationals without the specific approval of the National Manager, NTISS.

4. Extracts of information in this Instruction may be made as necessary. Such extracts shall be marked "FOR OFFICIAL USE ONLY," and shall not be made available to the general public without the specific approval of the National Manager, NTISS.

5. Federal departments and agencies shall implement this Instruction within 120 days of the effective date. It is requested that one copy of each department or agency implementing directive be forwarded to the National Manager, National Security Agency, ATTN: S04.


LINCOLN D. FAURER
Lieutenant General, USAF

FOR OFFICIAL USE ONLY

NTISSI No. 4001

CONTROLLED CRYPTOGRAPHIC ITEMS

1. REFERENCES. Reference is made within this Instruction to the following publications. The requirements of the references apply to this Instruction to the extent specified herein.

a. NACSI No. 4005, "Safeguarding and Control of Communications Security Material," dated 12 October 1979.

b. NACSI No. 4006, "Reporting COMSEC Insecurities," dated 20 October 1983.

c. NACSI No. 4010, "Routine Destruction and Emergency Protection of COMSEC Material," dated 23 February 1982.

d. NCSC-6, "National Policy Governing the Disclosure or Release of Communications Security Information to Foreign Governments and International Organizations," dated 16 January 1981.

e. NACAM-83/1, "Advisory Memorandum on Protection of Communications Security Information Released to Foreign Governments and International Organizations," dated 10 June 1983.

f. NCSC-9, "National Communications Security (COMSEC) Glossary," dated 1 September 1982.

NOTE: Several of the General COMSEC Doctrine (4000-series) and COMSEC Systems Doctrine (8000-series) NACSIs will require revision to accommodate the new Controlled Cryptographic Item (CCI) concept introduced by this Instruction. In the interim, where the requirements of a 4000- or 8000-series NACSI conflict with those of this Instruction, this Instruction shall take precedence.

2. PURPOSE AND BACKGROUND.

a. The new CCI category applies to specified, unclassified, secure telecommunications and information handling equipments, and associated cryptographic components. The intent is to promote the broad use of secure telecommunications and information handling equipments for the protection of national security (classified), as well as national security-related (unclassified) and other sensitive information which should be protected in the national interest.

FOR OFFICIAL USE ONLY

b. Secure telecommunications and information handling equipments, and associated cryptographic components, which are designated "Controlled Cryptographic Item," or "CCI," employ a classified cryptographic logic, and it is only the hardware or firmware embodiment of that logic which is unclassified. The associated cryptographic engineering drawings, logic descriptions, theory of operation, computer programs, and related cryptographic information remain classified.

c. Procedures for controlling CCI secure telecommunications and information handling equipments, and associated cryptographic components, are required to guard against preventable losses to an actual or potential enemy. However, in keeping with the spirit of expanded use of these equipments, minor lapses in carrying out control procedures shall be dealt with locally as a matter of administrative discretion. More serious infractions may constitute sabotage, loss through gross negligence, theft, or espionage that would be punishable under various sections of the United States Code or the Uniform Code of Military Justice.

3. APPLICABILITY. This Instruction applies to all departments and agencies of the U.S. Government, and their contractors, who handle, distribute, account for, store, or use CCI secure telecommunications and information handling equipments, and associated cryptographic components.

4. DEFINITIONS. The definitions contained in NCSC-9 apply to this Instruction, with the exception that the term "Controlled COMSEC Item (CCI)" as defined in NCSC-9 is replaced by the term "Controlled Cryptographic Item (CCI)" as defined below. Also given below are additional, special definitions which apply to this Instruction.

a. Controlled Cryptographic Item (CCI). A secure telecommunications or information handling equipment, or associated cryptographic component, which is unclassified but controlled. Equipments and components so designated shall bear the designator "Controlled Cryptographic Item" or "CCI."

b. Secure Telecommunications and Information Handling Equipment. Equipment designed to secure telecommunications and information handling media by converting information to a form unintelligible to an unauthorized interceptor and by reconverting the information to its original form for authorized recipients. Such equipments, employing a classified cryptographic logic, may be stand-alone crypto-equipments, as well as telecommunications and information handling equipments with integrated or embedded cryptography.

c. Cryptographic Component. The hardware or firmware embodiment of the cryptographic logic in a secure telecommunications or information handling equipment. A cryptographic

FOR OFFICIAL USE ONLY

component may be a modular assembly, a printed circuit board, a microcircuit, or a combination of these items.

5. RESPONSIBILITIES.

a. The Director, National Security Agency (DIRNSA), is responsible for:

(1) Determining which existing and future equipments and components are to be designated as CCI. (User departments and agencies may recommend equipments and components for designation as CCI. Such recommendations should include supporting documentation.)

(2) Establishing requirements for controlling CCI equipments and components.

(3) Ensuring that equipments and components designated as CCI are marked with the designator "CONTROLLED CRYPTOGRAPHIC ITEM" or "CCI."

(4) Issuing new or revised COMSEC system doctrine for equipment designated CCI.

b. The heads of departments and agencies are responsible for implementing procedures for controlling CCI secure telecommunications and information handling equipments, and associated cryptographic components, in accordance with this Instruction or other national issuances, as appropriate.

6. CONTROL REQUIREMENTS. The following subparagraphs set forth the minimum requirements for controlling unkeyed CCI equipments and components. Where such equipments and components contain classified key, they shall be protected in accordance with the requirements of NACSI No. 4005. Also, depending upon the application, other more stringent requirements may be prescribed.

NOTE: CCI equipment and components, when unkeyed, are unclassified and, therefore, do not fall under the purview of the Defense Industrial Security Program or the responsibilities of the Defense Investigative Service.

a. Access. A security clearance is not required for access to CCI equipments and components. However, access shall be restricted to U.S. citizens whose duties require such access. Access may also be granted to permanently admitted resident aliens who are U.S. Government civilian employees or active duty or reserve members of the U.S. Armed Forces whose duties require access. The provision of CCI equipment or components to foreign governments and international organizations is covered by NCSC-6 and NACAM-83/1.

b. Storage and Transportation. CCI equipments and components shall be stored and transported in a manner that affords protection at least equal to that which is normally provided to other high value/sensitive material, and ensures that access and accounting integrity is maintained.

c. Accounting. CCI equipments and components shall be accounted for at a central point within each department or agency as follows:

(1) CCI equipments shall be accounted for by serial number. Separate accountability is not required for CCI components installed in these equipments. Spare or other uninstalled CCI components shall be accounted for by quantity.

(2) The accounting system must provide the following:

(a) The identification of CCI equipments and components which are lost.

(b) Individual accountability in order to support prosecution in cases which involve infractions that would be punishable under the United States Code or the Uniform Code of Military Justice.

(3) CCI accounting data at the central point shall be made available to NSA via on-line or other readily accessible means.

d. Inventories. Within each organization that accounts directly to the central point, CCI equipments and uninstalled CCI components shall be inventoried at least annually. An inventory should also be accomplished whenever there is a change of personnel responsible for the safekeeping or accounting of an organization's holdings of CCI equipments and components. Inability to reconcile an organization's holdings of these equipments and components with the record of accountability at the central point shall be reported as an insecurity in accordance with NACSI No. 4006.

e. Reporting Insecurities. The insecurities reporting requirements of NACSI No. 4006 apply to CCI equipments and components.

f. Routine and Emergency Destruction. The routine and emergency destruction standards and procedures of NACSI No. 4010 apply to CCI equipments and components.

DISTRIBUTION:

NSA SPECIAL DISTRIBUTION

Plus:

NSC (ATTN: MR DEGRAFFENREID)
OMB (INTEL BRANCH NSD)
DUSD (P) (ATTN: DIR CI&SP AND DIR C2 POLICY)
DUSD (C3I) (ATTN: CDR PULFREY) (2)
OJCS (C3S) (2)
CSA (DAIM-OI) (2)
CSA (DAMI-CIC) (10)
CSA (DALO-SMC) (2)
CSA (DAMA-CSC) (2)
CNO (OP-941) (3)
CMC (OCT) (5)
HQ USAF (SITT) (5)
USCINOCENT (OCJ6-C) (2)
USCINCEUR (C3S) (2)
USCINCLANT (J6) (2)
HQ MAC (SI) (2)
USCINCPAC (C3S) (2)
USCINCRD (RCC4S-O) (2)
HQ SAC (SI) (2)
USCINCSO (J6) (2)
HQ SPACECOM (KR) (2)
COMUSFORCARIB (J6) (2)
COMUSFJAPAN (J6) (2)
COMUSFKOREA (J6) (2)
DIR ARFCOS (2)
DCSO (CODE B315) (20)
DIA (RCM-4) (10)
DIS (V0410) (5)
DLA (DLA-TI) (2)
DNA (LECD)
DIR TRI-TAC (TT-SC)
DIR TRI-TAC JTE (TT/TE-C)
CDR USAINSCOM (IAOPS-OP-P) (15)
CDR USACSLA (SELCL-NMP) (5)
CHNAVMAT (O8) (2)
COMNAVSEOCGRU (G-61) (15)
COMNAVELEXSYSCOM (PDE 110-231) (3)

DCMS (T60) (6)
 CG MCDEC (DEVGEN C3) (2)
 HQ TAC (SI) (2)
 HQ SISC (CK) (2)
 AFCSC (EPPP) (20)
 Dept. of Agriculture (MSD/FAS) (2)
 Dept. of Commerce (I&S) (2)
 Dept. of Energy (CSIM) (2)
 Dept. of Health & Human Services (IG) (2)
 Dept. of Interior (AMO) (2)
 Dept. of Justice (OIPR) (2)
 Dept. of State (ASC) (2)
 Dept. of Transportation (OI&S M-50) (2)
 Dept. of Treasury (ADTM) (10)
 CIA (OC-CSD) (2)
 CIA (DIR OIT) (2)
 CIA (OS MAIL) 2)
 CIA (OC/CSD/PSO) (2)
 DIR, IC STAFF (IIHC) (2)
 DIR, IC STAFF (DCI SECURITY COMMITTEE) (2)
 DIR, IC STAFF (POLICY AND PLANNING STAFF) (2)
 Drug Enforcement Administration (AIOC) (2)
 FAA (ADL-15) (6)
 FBI (TSD) (5)
 FCC (CODE 22800) (2)
 FEMA (RMIR-IM-TW-CS) (7)
 GSA (OIRM SECURITY MANAGER) (6)
 NASA (NIS-5) (CODE 100) (5)
 NCS (AO) (2)
 NRC (5721-MNBB) (2)

STAT

FOR OFFICIAL USE ONLY